

Decrets de l'Alcaldia

Decret. En ús de les facultats conferides a aquesta Alcaldia per l'art. 13.1 de la Carta de Barcelona, disposo:

Aprovar la Normativa tècnica per a la protecció de dades de caràcter personal en suport paper que dóna compliment al Reglament de desenvolupament de la Llei orgànica de protecció de dades (RLOPD), aprovat per Reial decret 1720/2007, de 21 de desembre.

Barcelona, 19 de març de 2012. L'alcalde, Xavier Trias i Vidal de Llobatera.
(Ref. Exp. 953/12)

NORMA TÈCNICA PER A LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL EN SUPORT PAPER A L'AJUNTAMENT DE BARCELONA

Aprovada el 3 de març de 2011 per la Comissió Tècnica de Seguretat en Protecció de Dades de Caràcter Personal (CSPD)

1. Objecte i àmbit d'aplicació

1.1. Aquesta norma tècnica té per objecte:

- a. Establir unes bones pràctiques que constitueixin els criteris generals d'aplicació de la normativa en protecció de dades de caràcter personal dels tractaments en suport paper o no automatitzats.
- b. Indicar les mesures de seguretat que cal implantar per tal de garantir la seguretat de les dades de caràcter personal i evitar-ne l'alteració, la pèrdua, el tractament o l'accés no autoritzats.
- c. Determinar els deures i obligacions del responsable executiu de fitxer (REF), del gestor operatiu de fitxer (GOF) i de la resta del personal implicat en els tractaments de dades de caràcter personal en suport paper.

1.2. Aquesta norma tècnica és d'aplicació al personal al servei de l'Ajuntament de Barcelona, dels seus organismes autònoms i de les entitats públiques empresarials. També al personal de les societats mercantils, consorcis i resta d'entitats on sigui majoritària, directament o indirecta, la representació de l'Ajuntament, quan exerceixin potestats públiques, les quals resten incloses, a efectes d'aquesta norma tècnica, dintre l'expressió "Ajuntament" o "Administració municipal".

A més, l'Ajuntament promourà que els criteris i principis que estableix aquesta norma tècnica siguin adoptats també per la resta de societats mercantils, organismes i entitats vinculades, així com per les empreses i entitats que gestionin serveis públics municipals.

1.3. Aquesta norma tècnica s'aplica a les dades de caràcter personal registrades en suport paper que les faci susceptibles de tractament, així com a tota modalitat d'ús posterior.

2. Conceptes

- a. **AIDA** (sistema AIDA): Sistema d'Administració Integral de la Documentació i dels Arxius de l'Ajuntament de Barcelona. El sistema AIDA estableix els criteris metodològics, tècnics i d'arxiu de l'Ajuntament de Barcelona. Els seus instruments bàsics són el Quadre de classificació, el Mètode de descripció i el Calendari de conservació.
- b. **Avaluació documental**: Procediment pel qual es determina la conservació o els terminis d'eliminació de la documentació de l'Administració municipal així com el seu règim d'accés. Actualment aquesta tasca està desenvolupada per la Comissió Municipal d'Avaluació i Accés a la Documentació.
- c. **Calendari de conservació**: Document que identifica les sèries o agrupacions documentals (que correspondrien en molts casos amb els fitxers automatitzats o no automatitzats) i les relaciona amb els seus terminis d'eliminació i condicions d'accés.

- d. **Cessió o comunicació de dades:** Tota revelació o difusió de dades realitzada a una persona diferent de la persona interessada.
- e. **Comissió Municipal d'Avaluació i Accés a la Documentació (CMAAD):** Òrgan col·legiat, tècnic i multidisciplinari encarregat d'avaluar els documents i determinar els terminis de conservació i el règim d'accés.
- f. **Dades de caràcter personal:** Qualsevol informació numèrica, acústica, gràfica, fotogràfica i alfabètica o de qualsevol altre tipus concernent a persones físiques identificades o identificables. Per ex.: noms, cognoms, DNI o altres combinacions identificatives, correu electrònic, professió, adreça, fotografies, etc.
- g. **Drets ARCO:** Drets d'accés, rectificació, cancel·lació i oposició, previstos per la normativa vigent en matèria de protecció de dades, l'exercici dels quals s'ha de garantir en els terminis, les condicions i els efectes establerts en l'esmentada normativa. Concretament, els anomenats drets ARCO són:
- Dret d'accés: Dret de les persones interessades a sol·licitar i obtenir gratuïtament informació de les seves dades de caràcter personal sotmeses a tractament, l'origen d'aquestes dades i les comunicacions efectuades o que es prevegin fer.
 - Dret de rectificació i cancel·lació: Dret de les persones interessades que siguin rectificades o cancel·lades, si escau, les dades de caràcter personal el tractament de les quals no s'ajusti a la legalitat vigent, especialment quan aquestes dades siguin inexactes o incompletes. D'acord amb la normativa aplicable, la cancel·lació comporta el bloqueig de les dades.
 - Dret d'oposició: Dret de les persones interessades a oposar-se al tractament de les seves dades de caràcter personal quan existeixin motius fonamentats i legítims, d'acord amb el que estableix la normativa vigent en matèria de protecció de dades.
- h. **Encarregat de tractament:** És la persona física o jurídica, pública o privada, que sol o conjuntament amb altres, tracta dades personals per compte de l'Ajuntament com a conseqüència de l'existència d'una relació jurídica que el vincula i delimita l'àmbit de la seva actuació per a la prestació d'un servei. Aquesta relació ha d'estar regulada en un contracte en què constin expressament totes les condicions i aspectes previstos a la normativa vigent, els quals es recullen als plecs de clàusules tipus.
- i. **Fitxer no automatitzat:** Conjunt de dades de caràcter personal organitzat de forma no automatitzada i estructurat d'acord amb criteris específics relatius a persones físiques, que permetin accedir sense esforços desproporcionats a les seves dades personals, ja sigui aquell centralitzat, descentralitzat o repartit de forma funcional o geogràfica.
- j. **Interessat/afectat:** Persona física titular de les dades que siguin objecte del tractament.
- k. **Mesures de seguretat:** Mesures de caràcter tècnic i organitzatiu necessàries per garantir la seguretat de les dades de caràcter personal i per evitar-ne l'alteració, pèrdua, tractament o accés no autoritzat. D'acord amb la normativa vigent, les mesures de seguretat exigibles als fitxers i tractaments de dades de caràcter personal es classifiquen en tres nivells (bàsic, mitjà i alt), en funció de les dades de què es tracti o de la finalitat que tinguin.
1. Nivell bàsic: Qualsevol fitxer o tractament de dades personals ha d'adoptar les mesures de seguretat de nivell bàsic.
 2. Nivell mitjà: A més de les mesures de seguretat de nivell bàsic, caldrà implantar mesures de nivell mitjà en els fitxers o tractaments municipals relatius a la comissió d'infraccions administratives o penals, en els fitxers que són responsabilitat de les administracions tributàries, i en els que ofereixen una definició de les característiques o de la personalitat dels ciutadans i que permeten avaluar determinats aspectes de la seva personalitat o del seu comportament.
 3. Nivell alt: A més de les mesures de seguretat de nivell bàsic i mitjà, s'implantaran mesures de seguretat de nivell alt als fitxers o tractaments

de dades de caràcter personal relacionats amb ideologia, afiliació sindical, religió, creences, origen racial, salut, vida sexual, violència de gènere i els que continguin o es refereixin a dades recollides per a finalitats policials sense consentiment de les persones afectades.

- l. **Quadre de classificació uniforme dels documents del sistema AIDA:** Sistema de classificació jeràrquic de la documentació basat en les funcions exercides per l'Ajuntament de Barcelona. El Quadre de classificació AIDA és una eina única i corporativa de l'Ajuntament de Barcelona.
- m. **Tractament de dades personals:** Totes les operacions i els procediments tècnics que permetin recollir, gravar, conservar, elaborar, modificar, utilitzar, consultar, bloquejar, suprimir i cancel·lar, així com les cessions de dades que derivin de comunicacions, consultes, interconnexions i transferències.
- n. **Usuari/ària:** Qualsevol persona física autoritzada per l'Administració municipal a accedir a dades o recursos.

3. Els fitxers amb dades de caràcter personal

3.1. Principi de qualitat de les dades

D'acord amb l'art. 4 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD), únicament es poden recollir i tractar les dades de caràcter personal que siguin adequades, pertinents i no excessives per a la correcta actuació administrativa o la tramitació del procediment administratiu corresponents. Aquestes dades només poden ser tractades amb la finalitat determinada, explícita i legítima per a la qual hagin estat recollides, en el marc de les competències i funcions que tingui atribuïdes l'Ajuntament.

Una vegada finalitzat el tractament o acomplerta la finalitat per a la qual hagin estat recollides, o quan hagin deixat de ser necessàries o pertinents, les dades de caràcter personal hauran de ser cancel·lades, llevat dels casos legalment autoritzats i d'aquells que així ho decideixi, d'acord amb la Llei, l'òrgan municipal competent en avaluació i accés documental. La cancel·lació implica el bloqueig de les dades, en els termes establerts en la normativa vigent en matèria de protecció de dades.

3.2. Principis d'informació i consentiment

D'acord amb l'art. 5 de la LOPD, quan es recullin dades de caràcter personal directament del les persones interessades mitjançant qüestionaris, formularis o altres documents similars, caldrà informar-los prèviament, de manera expressa, precisa i inequívoca, de l'existència d'un fitxer o tractament de dades de caràcter personal, de la finalitat de la recollida de les dades, dels destinataris de la informació, de la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició, i de la identitat i adreça de la persona responsable del tractament. Aquesta informació es facilitarà segons els procediments establerts per cada òrgan gestor.

Si la informació no es recull directament de la persona interessada, aquest haurà de ser informat també, dintre dels tres mesos següents al registre de les dades, del contingut del tractament i de la procedència de les dades, llevat que una llei digui el contrari o el tractament tingui finalitats històriques, estadístiques o científiques, o resulti impossible o exigeixi esforços desproporcionats, a criteri, en aquest darrer cas, de l'Autoritat Catalana de Protecció de Dades, prèvia consulta feta a través de l'òrgan competent de l'Ajuntament.

Quan així sigui necessari, caldrà a més obtenir de les persones interessades el seu consentiment per al tractament i, si escau, comunicació de les seves dades de caràcter personal, en la forma i casos establerts en la normativa d'aplicació i seguint el procediment establert per cada òrgan gestor.

3.3. Creació, modificació i supressió de fitxers

La creació, modificació o supressió d'un fitxer de titularitat municipal que contingui dades de caràcter personal s'haurà de fer per l'òrgan competent d'acord amb el que estableix la normativa vigent, i s'haurà de publicar i notificar amb l'antelació suficient a l'Autoritat Catalana de Protecció de Dades. Fins que no s'hagi

fet aquesta notificació no podrà iniciar-se ni la recollida de dades ni qualsevol altra operació de tractament de dades.

4. Mesures de seguretat

Caldrà adoptar les mesures de seguretat que corresponguin segons el tipus de dades de caràcter personal que siguin objecte de tractament, d'acord amb els requeriments especificats en el títol VIII del Reglament de desenvolupament de la LOPD (aprovat per Reial decret 1720/2007, de 21 de desembre, en endavant RLOPD), l'apartat 2 k) d'aquesta norma tècnica i els requisits i criteris que s'estableixen a continuació.

4.1. Mesures a adoptar pel que fa als expedients en tràmit o resultats que contenen dades de caràcter personal

4.1.1. L'expedient en tràmit

Durant la tramitació d'un expedient s'hauran de tenir presents les pautes o els criteris següents:

- a. Evitar la cessió o comunicació de dades de caràcter personal, llevat que aquesta estigui emparada per una llei o es tingui el consentiment de la persona interessada.
- b. Evitar fer reproduccions dels documents que s'inclouen als expedients, més enllà de les estrictament necessàries.
- c. Impedir que personal no autoritzat pugui accedir a la informació, mitjançant l'adopció de mesures adequades i proporcionades, que poden anar des de guardar els documents amb algun sistema de tancament a simplement donar la volta al full amb dades sensibles quan s'estigui en presència de personal no autoritzat.
- d. Guardar de forma segura els documents amb algun sistema que hi impedeixi l'accés durant l'absència del lloc de treball, malgrat sigui només per un moment. Els documents o fitxers que requereixen mesures de seguretat de nivell bàsic poden ser guardats en els armaris, despatxos, etc. més pròxims, mentre que els documents o fitxers que requereixen mesures de seguretat de nivell mitjà i alt han de ser guardats en armaris, arxivadors o altres elements dintre de zones reservades a personal autoritzat que estiguin tancades amb un sistema de clau o similar i sota control del personal amb responsabilitats de seguretat i arxiu.
- e. Custodiar i arxivar correctament els expedients o documents la tramitació dels quals és a càrrec del personal de l'òrgan gestor.
- f. Eliminar els esborranys i les còpies de forma segura ja sigui estripant els documents manualment o fent servir una destructora de paper que impedeixi la recuperació de la informació. L'eliminació de documents originals està regulada i no es pot fer sense el consentiment de l'organisme competent de l'Ajuntament, tal com es recull a l'apartat 4.5 d'aquest document.

4.1.2. La sortida dels documents

La sortida de documents que contenen dades de caràcter personal, via correu intern, missatgeria, etc., fora dels locals que estan sota el control de la persona responsable del fitxer o tractament, haurà de ser autoritzada. En el trasllat de la documentació s'hauran d'adoptar mesures dirigides a evitar la sostracció, pèrdua o accés indegut a la informació. En el cas de dades de caràcter personal a les quals corresponguin mesures de seguretat de nivell alt, se n'haurà d'impedir també la manipulació, a més de les situacions abans esmentades.

4.1.3. Identificació, classificació i inventari dels documents i expedients

Tot expedient o document ha de ser identificat, classificat i inventariat des del mateix moment en què és creat o rebut, d'acord amb els criteris establerts pel Sistema Municipal d'Arxius:

- La identificació s'ha de basar en una breu descripció del contingut de l'expedient a la seva caràtula. Aquesta descripció ha d'estar composta d'un títol, l'any de tramitació, el codi del Quadre de classificació AIDA, el número d'expedient i el nom de l'òrgan gestor. Pel que fa als expedients amb nivell de seguretat mitjà o alt, s'ha d'evitar, si és possible, que al títol de

l'expedient hi consti el nom de la persona interessada al costat de l'assumpte que s'hi tracta o altres dades de caràcter confidencial.

- La classificació ha de correspondre amb un codi del Quadre de classificació uniforme dels documents del sistema AIDA de l'Ajuntament de Barcelona.
- L'inventari dels expedients ha de contenir els títols dels expedients, la signatura topogràfica (número de caixa o qualsevol altre sistema que la identifiqui), l'any i el codi del Quadre de classificació AIDA. Cal fer un inventari per a cada sèrie o agrupació documental.

4.1.4. Arxivament i custòdia de documents i suports

L'arxiu dels documents i suports ha de garantir-ne la conservació, la localització i consulta; ha de facilitar-ne una possible recuperació futura i ha de fer possible l'exercici dels drets d'oposició, d'accés, de rectificació i de cancel·lació.

Un cop arxivat un expedient o document, s'hi ha d'impedir l'accés a personal no autoritzat.

L'arxivament dels documents i suports es farà d'acord amb els criteris de la direcció del Sistema Municipal d'Arxius i en el seu defecte, d'acord amb el que preveu la legislació.

Els documents i suports que continguin dades de caràcter personal s'han d'arxivar en armaris i dispositius dotats de mecanismes que n'obstaculitzin l'obertura. Quan això no sigui possible, caldrà adoptar mesures per impedir-hi l'accés de persones no autoritzades.

Els documents i suports amb dades personals que requereixin mesures de protecció de nivell mitjà o alt s'han d'arxivar en armaris, arxivadors o altres elements ubicats en àrees d'accés restringit, protegides amb portes dotades de clau o altres dispositius de tancament equivalents. Aquestes àrees han de romandre tancades quan no sigui necessari l'accés als documents.

La identificació dels documents i suports amb dades de caràcter personal als quals correspongui mesures de seguretat de nivell alt, es podrà fer amb sistemes d'etiquetatge comprensibles només per als usuaris autoritzats i no entenedors per a la resta de persones.

4.1.5. Criteris per a la correcta conservació dels documents

La localització i consulta de la documentació per part del personal autoritzat depèn en bona part de l'adopció d'unes correctes mesures de conservació. Les principals mesures de conservació que s'han d'adoptar són:

- a. Evitar fer malbé els documents. Certs elements nocius, com ara objectes metàl·lics o restes orgàniques, poden malmetre la documentació.
- b. Arxivar cada expedient amb els documents ordenats, indexats, foliats i amb una caràtula adient i fàcilment identificable, tal com estableix la legislació i d'acord amb les instruccions del Sistema Municipal d'Arxius.
- c. Evitar escollir per a l'arxiu una zona molt humida o d'excessiva calor i llum. Les condicions recomanables per als documents en paper estan entre 18-20 °C i 50% d'humitat relativa. En el cas que això no sigui possible, s'ha d'intentar establir uns paràmetres estables, d'acord amb els criteris que indiqui el Sistema Municipal d'Arxius.

4.1.6. Localització i consulta de la informació

La localització de la documentació s'ha de fer mitjançant l'instrument de recuperació d'informació més pertinent (inventari, catàleg, índex, etc.). L'instrument de recuperació forma un fitxer en si mateix i per tant té un nivell de protecció en funció del contingut. En qualsevol cas, sempre és d'accés lliure al gestor operatiu de fitxer, a la persona responsable de l'òrgan gestor, a l'encarregat de la tramitació dels expedients i a les persones amb responsabilitats de seguretat i arxiu. Cal distingir diferents tipus de consulta de la informació:

- a. Sol·licituds de consultes de documents fetes per l'Administració municipal en l'exercici de les seves funcions. Aquestes consultes tenen la consideració de tractament de dades, i les sol·licituds s'han d'adreçar a l'arxiu o a la persona responsable de l'òrgan gestor, segons pertorqui, els quals, en els casos de fitxers de nivells mitjà i alt, les registraran.
- b. Sol·licituds de consultes externes efectuades per persones físiques o jurídiques alienes a l'Administració municipal i diferents de la persona interessada. Llevat que qui les faci tingui la condició d'encarregat de

tractament, aquests accessos a la informació tenen la consideració de cessió o comunicació de dades. En tot cas, la persona sol·licitant haurà de justificar la seva petició i adreçar-la a la persona responsable de l'òrgan gestor o a l'arxiu si pertoca.

- c. Sol·licituds de consulta de persones afectades o interessades. Aquestes han d'anar adreçades a la persona responsable de l'òrgan gestor o a l'arxiu si pertoca, tot acreditant la identificació del sol·licitant.

Les sol·licituds d'accés només es podran denegar en aplicació de les limitacions legalment establertes. Les reclamacions i queixes referents a la negativa d'accés seran informades per l'òrgan municipal competent en avaluació i accés documental o altres òrgans competents.

L'Administració municipal ha de proporcionar de manera gratuïta i accessible la consulta i ha de posar els mitjans adequats per tal que aquesta es desenvolupi en unes condicions correctes, tant pel que fa a l'estat de la documentació com pel que fa a la sala o lloc de consulta.

4.1.7. Garantia de l'exercici dels drets d'accés, rectificació, cancel·lació i oposició

S'ha de garantir al ciutadà l'exercici dels drets d'accés, rectificació, cancel·lació i oposició al tractament de les seves dades personals. Aquests drets i la forma i lloc del seu exercici han d'aparèixer degudament indicats en tots els documents en què es demanin les dades personals als ciutadans.

Aquestes sol·licituds seran enviades directament a la Direcció d'Informació de Base i Cartografia (IMI), que s'encarregarà de tramitar-les al gestor operatiu de fitxer i d'assabentar-ne el responsable de seguretat corporatiu de tractament dels fitxers en suport paper.

D'acord amb la normativa aplicable, la resposta a aquestes sol·licituds no superarà els deu dies hàbils en el cas d'exercici dels drets de rectificació, cancel·lació i oposició, i d'un mes en el cas del dret d'accés.

4.2. Control d'accés a la documentació

El personal tindrà accés a aquells documents o expedients necessaris per al desenvolupament de les seves funcions.

El responsable executiu de fitxer o l'òrgan gestor ha de crear i mantenir una relació actualitzada d'usuaris i accessos autoritzats. També ha d'autoritzar els permisos d'accés eventuais. Les autoritzacions d'accés s'han d'assignar en base a les funcions encomanades.

El personal amb responsabilitats d'arxiu ha de controlar i registrar l'accés a la zona d'arxiu. L'exhaustivitat del registre serà proporcional al nivell de seguretat requerit pels fitxers i es farà d'acord amb els criteris que estableixi el Sistema Municipal d'Arxius. Com a norma general, només el personal amb responsabilitats d'arxiu accedirà a la zona d'arxiu.

En el cas dels fitxers als quals corresponguin mesures de seguretat de nivell alt, l'accés als documents es limitarà exclusivament al personal autoritzat, i caldrà establir mecanismes que permetin identificar els accessos realitzats en el cas de documents que puguin ser utilitzats per més d'un usuari. L'accés d'altres persones haurà de quedar adequadament registrat.

4.3. Còpies i reproduccions dels documents

A efectes d'aquest document, les còpies tenen el mateix tractament que els originals, ja que contenen la mateixa informació.

Les còpies hauran de ser destruïdes un cop hagin complert la finalitat per la qual van ser creades; les que no serveixin hauran de ser destruïdes al moment. Només es podran guardar aquelles còpies l'original de les quals no es tingui coneixement real d'on es troba.

Només les persones autoritzades podran fer còpies de documents amb dades de caràcter personal de nivell alt. Els noms de les persones autoritzades o el seu perfil hauran de ser recollits en un document i només podran fer les còpies necessàries.

En el cas de fitxers o tractaments de dades als quals corresponguin mesures de seguretat de nivell alt, la generació de còpies o la reproducció dels documents només podrà fer-se sota el control del personal autoritzat.

4.4. Mesures a adoptar sobre el trasllat massiu o transferència de documentació

4.4.1. Les transferències de documentació

Les transferències de documentació als centres d'arxiu del Sistema Municipal d'Arxius es regeixen pel reglament d'arxius i les directrius i terminis emesos pel Sistema Municipal d'Arxius i el Calendari de conservació i accés de la documentació.

L'òrgan gestor serà el responsable de la documentació fins que aquesta arribi al centre d'arxiu. Per aquesta raó ha de prendre les mesures de seguretat adequades i proporcionades en funció del nivell de seguretat de la documentació.

4.4.2. El trasllat massiu de documentació

El trasllat massiu de documentació amb dades personals, ja sigui per canvis d'ubicació d'oficina o altres motius, ha de ser autoritzat pel responsable de tractament o aquell en qui s'hagi delegat aquesta atribució.

En el trasllat de la documentació s'adoptaran les mesures adreçades a evitar la sostracció, pèrdua o accés indegut a la informació durant el transport. Entre d'altres mesures, caldrà inventariar la documentació, encapsar-la o introduir-la en contenidors amb sistema de tancament en cas de documents amb nivell de seguretat mitjà o alt, o adoptar altres mesures destinades a impedir l'alteració, pèrdua, robatori, manipulació o accés no autoritzat.

El trasllat es pot fer mitjançant el servei intern o un servei especialitzat. En ambdós casos, caldrà garantir la seguretat del trasllat i l'adopció de les mesures proporcionals als nivells de seguretat de la documentació que hagi de ser objecte de trasllat.

4.5. Mesures en l'eliminació de documents que contenen dades de caràcter personal

L'eliminació de documents originals es farà d'acord amb els terminis marcats pel Calendari de conservació i accés i d'acord amb els procediments establerts pel Sistema Municipal d'Arxius, en aplicació de la legislació en matèria de conservació d'arxius i documents i de la normativa sectorial aplicable en cada cas. A aquest efecte es pot demanar el suport i assessorament al mateix Sistema Municipal d'Arxius.

L'eliminació de còpies, fotocòpies i duplicats s'ha de fer d'acord amb la Instrucció sobre eliminació de documentació aprovada per la Comissió Municipal d'Avaluació i Accés a la Documentació.

Les eliminacions, tant si són documents originals com si són còpies, s'han de fer d'una forma segura per tal d'impedir la recuperació de la informació. Es pot portar a terme personalment (per exemple, estripant els documents manualment o fent servir una màquina destructora de paper) o es pot encarregar a una empresa externa mitjançant un contracte que inclogui el compliment de la legislació referent a la protecció de dades de caràcter personal i de la resta d'extremes recollits a l'art. 12 de la LOPD i art. 20 i següents del RLOPD. Aquesta empresa, que tindrà la consideració d'encarregat de tractament, haurà de ser especialitzada en la matèria i haurà de garantir l'eliminació mitjançant l'emissió del corresponent certificat.

4.6. Procediment de notificació, gestió i resposta davant les incidències

Es considerarà com a "incidències de seguretat" qualsevol anomalia que afecti o pugui afectar la seguretat de les dades de caràcter personal. El procediment a seguir per a la notificació d'incidències serà la següent:

1. L'usuari/ària comunicarà per escrit la incidència al cap de l'òrgan gestor o a l'encarregat de tractament responsable de seguretat.
2. L'òrgan gestor o encarregat de tractament adoptarà les mesures correctores necessàries.
3. L'òrgan gestor o encarregat de tractament comunicarà la incidència a la persona responsable de fitxer i a la persona responsable de seguretat.
4. La persona responsable de seguretat verificarà les mesures correctores i registrarà la incidència on hi constarà: el tipus d'incidència, el moment en què s'ha produït o detectat, la persona que fa la notificació, a qui es comunica, els efectes que se n'haurien derivat i les mesures correctores aplicades. En el cas de dades i fitxers als quals correspongui l'aplicació de

mesures de seguretat de nivell mitjà o alt, en el Registre hauran de consignar-se també els procediments de recuperació de les dades, indicant les dades recuperades i la persona que duu a terme aquesta recuperació, la qual haurà de ser prèviament autoritzada per fer-ho.

5. El responsable executiu de fitxer

El responsable executiu de fitxer és la persona amb càrrec de gerent o director que exerceix per delegació funcions del responsable de fitxer i que té les següents atribucions:

- a. Complir amb les obligacions que li imposi el responsable del fitxer en el compliment de les mesures de seguretat aplicables als fitxers que contenen dades de caràcter personal.
- b. Destinar els recursos, personal i finançament necessaris per a la protecció de la informació.
- c. Elaborar i implantar la normativa de seguretat detallant-la en el document de seguretat, així com les mesures de seguretat establertes reglamentàriament per a les dades de caràcter personal.
- d. Complir amb tots els requisits per a la protecció de la informació, tal com s'especifica en el document de seguretat, i en aquelles normes, directrius i procediments que la sostenen.
- e. Autoritzar l'accés de tercers a les dades de caràcter personal mitjançant encàrrecs de tractament o de prestació de serveis sense accés a les dades, tal com preveu el títol VIII del RLOPD.
- f. Assegurar que les funcions del responsable de seguretat i de l'usuari estan assignades adequadament, i designar, si escau, els responsables de Seguretat Sectorial que siguin necessaris.
- g. Assegurar que el personal ha estat informat i coneix aquesta política i aquelles normes, directrius i procediments que la sostenen, així com les conseqüències del seu incompliment.
- h. Reaccionar davant els riscos i altres aspectes que podrien suposar certa vulnerabilitat dels sistemes d'informació que hagin estat identificats.
- i. Assegurar la correcta implantació del circuit de resposta a les sol·licituds d'accés, rectificació, cancel·lació i oposició a les dades de caràcter personal.
- j. Designar, si escau, el gestor operatiu de fitxers, que durà a terme tasques de suport a l'execució d'aquestes obligacions i hauria de tenir un perfil de secretari tècnic-jurídic del sector o equivalent.
- k. Altres funcions que la persona responsable de fitxer li assigni.

6. Gestor operatiu de fitxer

El gestor operatiu de fitxer és la persona que actua per encàrrec del responsable executiu del fitxer i que té les següents atribucions:

- a. Proposar la normativa interna de seguretat requerida al document de seguretat, les mesures de seguretat establertes reglamentàriament per les dades de caràcter personal i el calendari per a la seva implantació.
- b. Proposar els procediments necessaris per complir amb els requisits per a la protecció de la informació, tal com s'especifica en el document de seguretat sectorial, i en aquelles normes, directrius i procediments que la sostenen.
- c. Proposar, si escau, el nomenament de les persones responsables de seguretat sectorials, per tal de garantir la implantació i documentació de la normativa interna i els procediments de seguretat abans indicats.
- d. Verificar que les funcions de la persona responsable de seguretat i de l'usuari/ària estan assignades adequadament, i informar el REF en cas necessari.
- e. Verificar que el personal ha estat informat i coneix la política de seguretat, les normes, directrius i procediments que la sostenen, així com les conseqüències del seu incompliment, i informar el REF en cas necessari.
- f. Informar el REF dels riscos i d'altres aspectes que podrien suposar certa vulnerabilitat dels sistemes d'informació que hagin estat identificats.
- g. Col·laborar en la resposta a les sol·licituds d'accés, rectificació, cancel·lació i oposició a les dades de caràcter personal i en la correcta implantació del

circuit d'atenció aprovat per la Comissió Tècnica de Seguretat en Protecció de Dades de Caràcter Personal.

- h. Mantenir en el document de seguretat una llista actualitzada i còpia dels contractes d'encarregat de tractament fets pel sector, garantint que inclouen, almenys, les clàusules relatives a protecció de dades incloses als plecs tipus.
- i. Altres funcions que el responsable executiu de fitxer li assigni.

7. El responsable de seguretat corporatiu de tractaments de documents en suport paper

La direcció executiva del Sistema Municipal d'Arxius és la responsable de seguretat dels tractaments dels documents en suport paper. En aquesta condició li corresponen les funcions següents:

- a. Vetllar per l'acompliment de les mesures de seguretat identificades en el document de seguretat, per verificar que es compleixen els procediments establerts en aquest.
- b. Actualitzar els mecanismes de seguretat establerts perquè es compleixin, en tot moment, segons la legislació vigent en matèria de seguretat de dades de caràcter personal.
- c. Notificar totes aquelles circumstàncies que detecti i afectin el document de seguretat o l'exercici dels drets fonamentals dels afectats.
- d. Participar en els nous desenvolupaments que es produeixin per assegurar que compleixen amb les mesures de seguretat requerides pel RLOPD.
- e. Analitzar les conclusions de l'informe d'auditoria de compliment dels requisits establerts en el RLOPD i trametre-les al responsable.
- f. Participar en les accions de divulgació del document de seguretat dutes a terme pel responsable del fitxer.
- g. Notificar totes les incidències detectades amb un possible efecte sobre la protecció de dades.
- h. Proposar al responsable de fitxer les mesures divulgatives a adoptar quan es consideri necessari.
- i. Altres funcions que el responsable executiu de fitxer li assigni.

8. Drets i obligacions del personal

8.1. Drets del personal

- a. Consultar i rebre informació i formació sobre els criteris de seguretat dels documents, fitxers i tractaments en suport paper que siguin d'aplicació en funció del lloc de treball, i sobre els procediments, aplicacions i canals d'incidència.
- b. Disposar de les eines, mecanismes i procediments per a un ús adequat dels documents, fitxers i tractaments en suport paper amb dades de caràcter personal.
- c. Disposar d'un canal d'assistència per a la resolució dels dubtes generats i d'un canal de comunicació de les possibles incidències de seguretat que hagi detectat o que hagi tingut coneixement en relació amb els documents, fitxers i tractaments en suport paper.

8.2. Obligacions del personal

- a. Conèixer i observar totes les mesures, normes, procediments, regles i estàndards que afecten les funcions que desenvolupa pel que fa al tractament de dades de caràcter personal en suport paper i a la seva comunicació.
- b. Notificar al responsable executiu del fitxer o al responsable de seguretat les incidències de seguretat de les quals tingui coneixement respecte als recursos protegits, segons els procediments establerts en aquest document, especialment en l'apartat de "Procediments de notificació, gestió i resposta davant les incidències".
- c. Mantenir secret i confidencialitat de les dades personals conegudes en el desenvolupament de les seves tasques, fins i tot després de la finalització del contracte o relació amb l'Ajuntament, ja sigui aquesta de naturalesa funcional, laboral o de qualsevol altre tipus.

- d. No crear documents ni fitxers que continguin dades de caràcter personal, ni fer tractaments, cessions o comunicacions d'aquestes dades llevat dels casos autoritzats per l'òrgan gestor.
- e. Evitar l'accés per part de personal no autoritzat a aquelles dades o documents que es trobin sota la seva responsabilitat i que encara no s'hagin incorporat a l'espai d'arxiu.
- f. Evitar la visibilitat o accés a informacions amb dades de caràcter personal durant l'absència del lloc de treball, independentment del temps d'absència, i deixar ordenat l'espai de treball.
- g. Aplicar els criteris d'arxiu, còpia, eliminació, accés i consulta establerts per la direcció del Sistema Municipal d'Arxius, amb el suport de l'arxiver/a referent del seu àmbit.
- h. Tenir identificada i inventariada la documentació sota la seva responsabilitat aplicant els criteris d'arxiu establerts per la direcció del Sistema Municipal d'Arxius.
- i. Fer servir únicament les dades que necessiti per al correcte desenvolupament de la seva feina i destinar-les a la finalitat per a la qual van ser recollides.
- j. Evitar el trasllat, enviament o treball amb documentació que conté dades personals fora dels espais de treball sense consentiment del cap de l'òrgan gestor o del responsable executiu de fitxer. En el seu cas, a més de l'autorització, caldrà que s'adoptin les mesures de seguretat necessàries, en funció del nivell de protecció que requereixin les dades.
- k. Comunicar qualsevol incidència relacionada amb el tractament de dades de caràcter personal, com ara pèrdues, sospites d'ús indegut, recuperació de dades, etc., per les vies de notificació d'incidències que s'estableix en aquest document, o que indiqui l'òrgan competent.
- l. Les altres obligacions que es derivin de la normativa aplicable i d'aquest document.

A més a més, **el personal amb responsabilitats d'arxiu** també haurà de complir les obligacions següents:

- a. Actuar sota les directrius del responsable executiu de fitxer.
- b. Vetllar per la custòdia dels documents que es troben dintre dels espais que estiguin sota la seva responsabilitat.
- c. Aplicar els criteris d'arxiu, còpia, eliminació, accés i consulta establerts per la direcció del Sistema Municipal d'Arxius, dintre dels espais que estiguin sota la seva responsabilitat, amb el suport de l'arxiver/a referent del seu àmbit.
- d. Vetllar per l'aplicació dels criteris d'arxiu, còpia, eliminació, accés i consulta establerts per la direcció del Sistema Municipal d'Arxius, per part del personal que gestiona els documents que més tard passaran al seu control, amb el suport de l'arxiver/a referent del seu àmbit.
- e. Portar un control dels accessos a la zona que estiguin sota la seva responsabilitat i als documents que hi siguin custodiats, i mantenir un registre d'accessos per als casos de fitxers amb dades de nivell alt.
- f. Mantenir una relació actualitzada d'usuaris o perfils d'usuaris amb accés autoritzat als espais que es trobin sota la seva responsabilitat.

Disposicions addicionals

Primera. Actualització del document

La direcció executiva del Sistema Municipal d'Arxius, com a responsable de seguretat corporatiu dels tractaments de documents en suport paper, proposarà a la Comissió Tècnica de Seguretat de Protecció de Dades les actualitzacions o modificacions d'aquest document que consideri necessàries.

Segona. Incompliment

L'incompliment dels deures i obligacions establerts en aquesta norma tècnica, així com les responsabilitats que se'n puguin derivar, pot comportar l'aplicació del règim disciplinari corresponent.

* * *